

On page 15, replace the page number with the following:

--32--.

On page 16, replace the page number with the following:

--33--.

On page 17, replace the page number with the following:

--34--.

On page 18, replace the page number with the following:

--35--.

On page 19, replace the page number with the following:

--36--.

On page 20, replace the page number with the following:

--37--.

On page 21, replace the page number with the following:

--38--.

**IN THE ABSTRACT**

On page 20, replace the page number with the following:

--39--.

**REMARKS**

Entry and consideration of the Preliminary Amendment is respectfully requested.

Preliminary Amendment is being filed to correct typographical errors and to more clearly identify the claimed invention. No new matter has been introduced. Upon entry of this

Preliminary Amendment, claims 1-58 will be pending in this application, and there will be 39 pages in total for the specification including claims and Abstract. Entry of this Preliminary Amendment and examination on the merits is respectfully requested.

The attached to this Amendment (entitled as Attachment I) shows the amendments made to the specification, claims 1, 27, 28, and 30 and the Abstract by bracketing the text that has been deleted and underlining the text that has been added.

**AUTHORIZATIONS**

The Commissioner is hereby authorized to charge any additional fees which may be required for timely consideration of this response, or credit any overpayment to Deposit Account No. 13-4503, Order No. 4208-4034US2.

Respectfully submitted,  
MORGAN & FINNEGAN, L.L.P.

Dated: 11/20/02

By: Mark D. Pratt  
Mark D. Pratt  
Reg. No.: 45,794  
(202) 857-7887 Telephone  
(202) 857-7929 Facsimile

**CORRESPONDENCE ADDRESS:**

Morgan & Finnegan  
345 Park Avenue  
New York, NY 10154

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Serial No. : 10/051,249                      Group Art Unit: 2131  
Filed : January 22, 2002                      Examiner: to be assigned  
For : A Method, System And Computer Program Product For Secure  
Ticketing In A Communications Device

**ATTACHMENT**

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Please note the following amendments to the specification, claims 1, 27, 28 and 30 and

Abstract:

**IN THE SPECIFICATION**

Between pages 4 and 5, please note the following changes to paragraph No. 0010:

--[0010]        Therefore, it is desirable to provide a system, method and computer program product that provides secured ticketing in a [personal] communications device, such as e.g., personal trusted device using a tamper-resistant security element. The system, method and computer program product of the embodiment of present invention disclosed herein address this need.--

Between pages 5 and 6, please note the following changes to paragraph No. 0015:

--[0015]        The accompanying figures illustrate the details of the method, system and computer program product of an embodiment of the present invention for implementing secure ticketing in a [communication] communications device. Like reference numbers and

designations in these figures refer to like elements.--

On page 6, please note the following changes to paragraph No. 0018:

--[0018] Fig. 3 is a detailed diagram that illustrates a [communication]  
communications device in accordance with an embodiment of the present invention.--

Between pages 7 and 8, please note the following changes to paragraph No. 0023:

--[0023] The mobile equipment **102** is in communication with the security element **103** via the bus **109**. Additionally, the personal trusted device **100** is in communication with third-party devices **140**, **150**, [and] **160** for receiving and transmitting electronic tickets via a connection **111**, which is typically, but not necessarily a wireless connection. Examples of the communication links may comprise e.g., GSM, GPRS, WCDMA, DECT, WLAN, PSTN, ISDN, ADSL and xDSL connections or the DOCSIS return channel in a cable TV environment, or any short range connection like Bluetooth, IrDA. Communication between the mobile equipment **102**, external memory **106** and third-party devices **140**, **150** and **160** is achieved using various protocols executed by the operating system **107** and the central processor **210**. The protocols used for communication between the mobile equipment **102**, the security element **103** and third-party devices **140**, **150**, **160** include, in an embodiment, a request and store ticket protocol, a use ticket protocol and a check ticket protocol.--

On page 8, please note the following changes to paragraph No. 0024:

--[0024] The personal trusted device **100** in Fig. 1 is connectable to, for example, a wireless network **116** via a transmitted signal such as a frequency-modulated signal from the personal trusted device **100** and received by a base station antenna **114**. It will

be understood that the mobile equipment 102 may be provided also with the short range connectivity in addition to the mobile communication activity. From the wireless network 116, the personal trusted device can be connected to various third-party devices 140, 150, 160 via a network 130 and a wireless network switch 120. The network 130 can be a server, Intranet, Internet, public switching network (PSTN), public exchange (PBX) or the like. The user (not shown) of the device can communicate with the personal trusted device 100 using the display 212 and keypad 104 [and] via the bus 109.--

On page 10, please note the following changes to paragraph No. 0028:

--[0028] Every ticket has a signature, which can be verified using the public key of the issuer of the ticket. Because all tickets in the example have been issued by different issuing devices they have different signatures and the signatures can be verified using the public key of the issuing device. When the ticket is presented to a collecting device, the collecting device checks the validity of the ticket by verifying the signature in the ticket. The first ticket is associated with the counter ID "12345" and it is issued by "Grey Hound [hound] Co." for ten (10) uses. Correspondingly, the ticket associated with the counter ID "12347" is issued by the cinema company "stardust" for three (3) uses. The additional information can specify the rights as in the example for the ticket issued by the "[state] State Filharmonic" to a certain date and to a certain seat. If the "counter value" stored in the security element is compared with the value "N" in the ticket, it can be seen that the user having a ticket with a counter ID "12345" has used "Greyhound Co." services five (5) times and can still use the services of "Greyhound Co." for another five (5) times.--

On page 11, please note the following changes to paragraph No. 0029:

--[0029] Figure 2 illustrates in more detail the [cyptography] cryptography for implementing secured ticketing by mobile equipment **102**, the security element **103**, and third-party devices **140**, **150**, **160** in accordance with an embodiment of the invention. The mobile equipment **102** stores ticket data **101A** in the internal storage device **101** of the personal trusted device **100**. The ticket data **101A** corresponds to the valid tickets received [by] from the issuing device **140** and not yet redeemed by the user. More importantly, the [external] security element **103** is trusted by the third parties involved. The security element **103** uses the public key **103C** and a corresponding private key **103D** only to implement a trusted counter application. Additionally, the mobile equipment **102** may also request a manufacturer certificate **103B** to ensure that the external security device **103** is issued by a trusted manufacturer.--

Between pages 11 and 12, please note the following changes to paragraph No. 0031, please note the following:

--[0031] The third-party devices contemplated by the invention include issuing devices **140**, collecting devices **150**, and checking devices **160**. The issuing device is used to send electronic tickets to the user of the personal trusted device **100** after the payment of third-party services. Additionally, the collecting device **150** is used to redeem electronic tickets and the checking device **160** is used to [periodically] check if the user is in possession of a correctly redeemed ticket. Each of the third-party devices includes public and private keys **140A**, **140B**, **150A**, **150B**, **160A**, **160B**. It is presumed that the personal trusted device **100** is trusted by the user but is not trusted by the third-party devices. Thus, each of third-

party devices can use public and private keys **140A, 140B, 150A, 150B, 160A, 160B** to encrypt critical data for secure communication of electronic tickets with the personal trusted device **100**. The keys **140A, 140B, 150A, 150B, 160A, 160B** in the third-party devices can be encryption keys, signature keys or master keys. A master key is a common symmetric key shared by all issuing, collecting and checking devices **140, 150, 160**.--

Between pages 12 and 13, please note the following changes to paragraph No. 0034:

--[0034] Fig. 4 illustrates the steps involved for executing the request and store ticket protocol that is used for receiving and storing electronic tickets in the personal trusted device **100**. Initially, in step **S1** mobile equipment **102** requests the card certificate **103B** stored in the [external] security element **103**. In another embodiment of the invention the card certificate itself is not stored in the security element **103**, but a pointer to the card certificate in the form of an URL address is stored in the security element **103**, wherein in step **S1** the mobile equipment **102** requests the card certificate from the URL. As mentioned previously, the certificate ensures that the security element **103** is issued by a trusted manufacturer. In step **S2** the security element **103** sends a card certificate **103B**, which is verified by the mobile equipment **102** as a compliant card using a certificate chain. Two certificates can be used in order for mobile equipment **102** to verify that the security element **103** possesses a compliant card certificate **103B**. For example, a certificate issued by the mobile equipment **102** to the manufacturer of the security element **103**, and a compliant card certificate issued by the manufacturer of the [external] security element **103** to the security device **103** itself. In step **S2**, the security element **103** also sends a public key **103C** or the card certificate **103B**. In step **S3**, the mobile equipment **102** issues a create counter request to create a new counter to

correspond to the electronic ticket that is to be received and later redeemed and/or checked by third party devices **140, 150, 160**. In step **S4**, the security element **103** sends a counter ID that is used to uniquely identify a counter. In step **S5**, the mobile equipment **102** forwards the counter ID, and the public key and manufacturer certificate of the external security element **103** to the issuing device **140**. In step **S6**, the issuing device **140** creates a ticket. The ticket is a signature on authenticator data for the issuing device consisting of the counter ID **103A**, the public key **103C** and a number of uses **N** (not shown) of the ticket created. The number of uses is, for example, the number of uses allowed by the user for this ticket (e.g., 10-use ticket will have **N=10**). In addition, the authenticator data may include other relevant information, such as e.g., a seat number and/or a date and/or time related to the ticket, to be used by the personal trusted device **100**. By way of example, the ticket issued using the issue ticket protocol resembles  $\text{ticket} = \text{Sig\_Issuer}(\text{counterID}/\text{Public Key\_Device } 103/\text{N}/\text{other\_info})$ . In step **S6**, the ticket is sent to the mobile equipment **102** and stored in the internal storage device **101**.--

On page 14, paragraph No. 0035, please note the following changes:

--[0035]        If the issuing device **140** wants to further determine the authenticity of the security element **103**, and the ticket data **101A**,[,] [The] the issuing device **140** can issue a challenge to the mobile equipment **102** prior to creating the ticket. In this case, the mobile equipment **102** responds to the challenge by invoking a read counter request and returns a signature on authenticator data for the [external] security element **103** that includes the current counter value. If the signature and data are verified as correct, then the issuing device **140** will create and issue a valid ticket.--



Between pages 15 and 16, please note the following changes to paragraph No. 0040:

--[0040]       The ticket issued by an issuing device 140 can also include a [multi-used] multi-use ticket. In the case of a multi-used ticket, the mobile equipment 102 may send both the original ticket as well as the set of validated tickets obtained from the collecting device 150. The collecting device 150 would then use the additional information (i.e., validated tickets) to make decisions with regard to access control. Additionally, a collecting device 150 may also replace an old ticket or issue a new ticket. To this end, a collecting device 150 also acts as an issuing device 140.--

On page 16, please note the following changes to paragraph No. 0041:

--[0041]       Fig. 6 illustrates the check ticket protocol in accordance with an embodiment of the invention. In step S15, the mobile equipment 102 sends a ticket to the checking device 160. In step S16, the checking device 160 sends a challenge to the mobile equipment 102. In step S17, the mobile equipment 102 invokes a read counter for the corresponding counter ID by sending a read counter request to the [external] security element 103 using the challenge of the checking device 160 as an input parameter. In step S18, the security element 103 sends an authorization token that contains the current value of the counter to the mobile equipment 102. By way of example, the authorization token sent using the check ticket protocol is AuthToken = Sig\_Device 103 (Read\_Response/CounterID/Challenge/current\_value). In step S19, the mobile equipment 102 forwards the authorization token from the security element 103 to the checking device 160. The checking device 160 checks the current value of the counter using the public key 103C. In step S20, the checking device 160 sends an acknowledgment to the mobile

equipment 102 indicating the status of the check. The status of the check by the checking device 160 is either success or failure.--

On page 18, please note the following changes to paragraph No. 0047:

--[0047]        Additionally, as an alternative to computing an authorization token, a MAC can be used as an authentication method. For example, the MAC can be a code function such as HMAC-MD5 with the public key 103C as the key of the MAC function. By way of example, the issue ticket protocol would change as follows if a MAC function is used as an authentication method. In response to a ticket request, the issuing device 140 creates a ticket and also computes an encrypted key (EncKey) by encrypting the counter ID and MAC key (MACKey) using the public encryption key 103C for the security element 103. By way of example, the ticket issued using the issue protocol and the MAC is Ticket = Sig\_Issuer (CounterID/Public Key\_Device 103/N/Other\_Info), EncKey = Enc\_device 103(CounterID/MACKey). The mobile equipment 102 inputs the received encrypted key EncKey into security element 103. The security element 103 recovers the MACKey from the EncKey and sets the authentication method to MAC using MACkey. The security element 103 sends an acknowledgment to the mobile equipment 102. Other protocols would have similar changes as noted above if a MAC is used as an authentication method.--

#### **IN THE CLAIMS**

Please note the following changes to claims 1, 27, 28, and 30:

--1. (Amended)        A system for secure ticketing in a communications device, comprising:

a mobile equipment that includes a first storage device;

a security element that includes a second storage device;  
at least one third-party device; and  
a processor in communication with said first storage device, said second storage device and said third-party device configured to:  
authenticate said security element;  
[created] create and initiate at least one counter stored in said second storage device in said secure element;  
receive at least one electronic ticket from said third-party device and storing said at least one electronic ticket in said first storage device;  
redeem said at least one electronic ticket stored in said first storage device with said at least one third-party device; and  
update a counter value for the counter in said second storage device to correspond to the redemption of said electronic ticket with said third-party device.

27. (Amended) A computer program product for secured ticketing in a communications device, comprising:  
a computer readable medium;  
program code in said computer readable medium for authenticating a security element;  
program code in said computer readable medium for creating and initiating at least one counter in said security element;  
program code in said computer readable medium for requesting at least one electronic ticket from at least one third-party device;

program code in said computer-readable medium for storing said electronic ticket from said at least one third-party device in a storage device of said communications device;

program code in said computer-readable medium for redeeming said at least one electronic ticket stored in said storage device with at least one third-party device; and

program code in said computer readable for updating a counter value in said security element to correspond to redemption of said at least one electronic ticket with at least one third-party device.

28. (Amended) A method of requesting, creating, and storing a ticket for secure ticketing in a system comprising a mobile equipment having a first storage device, a secure element having a security element comprising a second storage device with a certificate and a pair of encryption keys, and at least one third-party device having a cryptographic master public key and configured to issue tickets, the method comprising:

authenticating the said security element;

creating and initiating at least one counter in said security element;

requesting at least one ticket from said third-party device;

creating at least one ticket by the said third-party device;

receiving at least one ticket from the said third-party device, and

storing the said at least one ticket received in the first storage device.

30. (Amended) The method of claim 28, wherein said creating and initiating at

least one counter comprises:

said mobile equipment sending a request to create a counter in the security element;  
said security element creating a counter by giving a unique counter ID, and initializing  
the counter to zero; and  
said security element sending the created counter ID to said mobile equipment.--

Please note the following amendments to the page numbers of the Claim Section:

On page 2, please note the following change to the page number:

--[2]19--.

On page 3, please note the following change to the page number:

--[3]20--.

On page 4, please note the following change to the page number:

--[4]21--.

On page 5, please note the following change to the page number:

--[5]22--.

On page 6, please note the following change to the page number:

--[6]23--.

On page 7, please note the following change to the page number:

--[7]24--.

On page 8, please note the following change to the page number:

--[8]25--.

On page 9, please note the following change to the page number:

--[9]26--.

On page 10, please note the following change to the page number:

--[10]27--.

On page 11, please note the following change to the page number:

--[11]28--.

On page 12, please note the following change to the page number:

--[12]29--.

On page 13, please note the following change to the page number:

--[13]30--.

On page 14, please note the following change to the page number:

--[14]31--.

On page 15, please note the following change to the page number:

--[15]32--.

On page 16, please note the following change to the page number:

--[16]33--.

On page 17, please note the following change to the page number:

--[17]34--.

On page 18, please note the following change to the page number:

--[18]35--.

On page 19, please note the following change to the page number:

--[19]36--.

On page 20, please note the following change to the page number:

--[20]37--.

On page 21, please note the following change to the page number:

--[21]38--.

**IN THE ABSTRACT**

On page 20, please note the following change to the page number:

--[22]39--.